IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiffs, vs. ISAIAH BROWN, WAKONDA HAZEL, and BAJAH PITTMAN, Defendants.	**4:17CR3004** **FINDINGS AND RECOMMENDATION**

Pending before the court are Motions to Suppress filed by Defendants Isaiah Brown, Wakonda Hazel, and Bajah Pittman. (Filing Nos. 134, 136, & 138). The defendants seek to suppress historical cell-site location information and related evidence compiled and obtained by the government through 18 U.S.C. §2703(c) & (d).

BACKGROUND FACTS

Between January 2014 and April 2016, several bank larcenies and attempted bank larcenies were committed in which the suspects pulled and dragged automatic teller machines ("ATMs") through broken glass doorways and windows with chains, ropes, or other cables attached to stolen vans or pickup trucks.

On November 23, 2015, one such bank larceny was committed in the lobby of First State Bank in Waverly, Nebraska. Bank surveillance video revealed multiple suspects. One of the suspects appeared to be using a cellular telephone while at the ATM. The Lancaster County Sheriff's Office ("LCSO") and the Lincoln Police Department ("LPD") conducted analysis of the video surveillance

tapes and cellular tower data, and with telephone record analysis, identified Darnell Gordon and Cal McCoy as suspects in the incident. On the same day, Gordon was arrested for driving with a suspended license. After the arrest, LCSO reported that Gordon made jail calls to several individuals, including numerous calls to a cellular telephone number ending in 8674 which was subscribed to Defendant Wakonda Hazel.

LPD conducted additional telephone analysis and received pen registers for Gordon's phone. The analysis and records revealed frequent calls between Gordon and a telephone number ending in 1358 which was subscribed to Defendant Isaiah Brown. Brown had been previously arrested in 2014 for burglary and possession of a stolen ATM.

On March 27, 2016, Douglas County Sheriff's Office ("DCSO") conducted a traffic stop on a blue 2011 Hyundai Sonata, a 2016 Chevrolet HHR SUV, and a stolen white pickup truck near Fremont, Nebraska. The Sonata was registered to Defendant Bajah Pittman. Occupants of the vehicles were Hazel, Darnell Gordon, Lyle Gordon, and Kentrell Reed. Each occupant was arrested and on March 29, 2016, Pittman was arrested for conspiracy to commit a felony. A search warrant was executed on her cell phone which has a number ending in 0844.

Based upon the above facts, as part of its investigation, the United States Attorney's Office applied for and received orders seeking the disclosure of cell phone records, including subscriber name, call information, telephone or instrument numbers, user activity records, and cell tower data for certain time periods for phone numbers ending in 8674, 0844, and 1358. (See Exhs. 3A, 5A, & 7A). These numbers were subscribed to Defendants Hazel, Pittman, and

Brown respectively. The undersigned magistrate granted each order pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(c) & (d).

With the defendants' historical cell-site information,[1] the Federal Bureau of Investigations ("FBI") compiled the defendants' information for the specific robbery dates and created maps showing whether defendants' individual phones were active within close proximity (in location and time) to the robberies. (See Defense Exh. 3). For an example, the historical cell-site location data received from Sprint regarding Defendant Hazel's cell phone showed that her phone actively used Sprint towers 93, 94, & 96 which were respectively located 5.2 miles north of, 4.9 miles south of, and 6.8 miles southeast of the Nehawka Bank on the September 25, 2015 robbery date; the activity consisted of phone calls received from co-defendants Brown and Darnell Gordon.

---

[1] As outlined in several other cases including, United States v. Carpenter,

> [C]ellphones work by establishing a radio connection with nearby cell towers (or "cell sites"); . . . individual towers project different signals in each direction or "sector," so that a cellphone located on the north side of a cell tower will use a different signal than a cellphone located on the south side of the same tower. . . . [C]ell towers are typically spaced widely in rural areas, where a tower's coverage might reach as far as 20 miles. In an urban area like Detroit, however, each cell site covers "typically anywhere from a half-mile to two miles." . . . [W]ireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites where the call began and ended.

819 F.3d 880, 885 (6th Cir. 2016); see also United States v. Jones, 908 F. Supp. 2d 203 207–08 (D. D.C. 2012). "This information is referred to as historical cell-site information. . . . Historical cell-site information includes the time a call or text message is made or received; the telephone numbers involved in the communication; the cell tower information (including its location); and the duration of the call." Jones, 908 F. Supp. 2d at 208. And the term "historical cell-site location information" specifically refers to the location of the cell tower utilized by the subscriber's phone.

In total, the collected data and maps showed: Defendant Hazel's phone was active the vicinity of the robberies of the Nehawka Bank in Union, Nebraska on September 25, 2015; the Casey's Convenient Store in Des Moines, Iowa on October 8, 2015; and the First State Bank in Waverly, Nebraska on November 23, 2015. Defendant Brown's phone was active in the vicinity of the robberies of Nehawka Bank in September, 2015 and Casey's Convenient Store in October, 2015. Defendant Pittman's phone was active in the vicinity of the First State Bank robbery in November, 2015.

On January 19, 2017, Defendants Isaiah Brown, Bajah Pittman, Wakonda Hazel, and seven co-defendants were indicted by a federal grand jury. (Filing No. 1). The indictment charges the defendants with a wide-ranging conspiracy to commit bank larceny and attempted bank larceny of ATM machines from January 2014 to April 2016, sometimes by using stolen vehicles.[2] The indictment alleges some of the defendants, as part of the conspiracy, "conducted visual surveillance of the areas around businesses with ATM machines to attempt to detect the possible presence of law enforcement, while other defendants broke and entered into the businesses and removed the ATM machines." (Filing No. 1). The indictment additionally alleges "it was also part of the conspiracy that defendants utilized cellular telephones to monitor the location of local law enforcement in relation to the business where the ATM machines were located, while the defendants attempted to remove the ATM machines from the businesses." Id.

On June 2, 2017, Brown, Pittman, and Hazel filed the instant motions to suppress. (Filing Nos. 134, 136, & 138).

---

[2] , The charges included conspiracy to commit bank larceny, in violation of 18 USC §§ 371 and 2113(b), four counts of bank larceny, in violation of 18 USC § 2113(b), and one count of interstate transportation of a stolen motor vehicle, in violation of 18 USC §§ 2312, 2314 and 2.

ANALYSIS

Defendants Brown, Pittman, and Hazel each seek to suppress evidence of historical cell-site location data obtained through the orders pursuant to 18 U.S.C. § 2703(c) & (d). They argue the disclosure of their cell-site location information was in violation of the Fourth Amendment.

The Fourth Amendment guarantees citizens the right to be free from unreasonable searches and seizures. U.S. Const. amend. IV. Rakas v. Illinois, 439 U.S. 128, 143 (1978); Katz v. United States, 389 U.S. 347, 361 (1967). A defendant who challenges a search or seizure under the Fourth Amendment must have a reasonable expectation of privacy in the area searched or the items seized, with the defendant bearing the burden of proving that threshold issue. Rawlings v. Kentucky, 448 U.S. 98, 104–05 (1980). Only where the Fourth Amendment has been violated should a party "benefit from the [exclusionary] rule's protection." Rakas, 439 U.S. at 134.

In assessing whether the Fourth Amendment is implicated, the court must first examine "the nature of the state activity that is [being] challenged." Smith v. Maryland, 442 U.S. 735, 741 (1979). In this case, the challenged activity is the Government's acquisition of historical cell-site location records for each defendant from their respective cellular phone service providers. In each instance, the Government sought and received orders pursuant to the SCA,18 U.S.C. § 2703(d), for the disclosure of cell phone records, including historical cell-site location data. And the service providers, as the custodian of the records, produced the records pursuant to those orders. (See Gov. Exhs. 3B, 5B, & 7B).

The SCA provides that to gain access to these non-content records (records which do not include the content of any communications between the defendant and another), the Government must either obtain a warrant by demonstrating probable cause or a court order by demonstrating "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Defendants Hazel, Pittman, and Brown do not argue that the government failed to meet the standards for a 2703(d) order. Instead, they argue historical cell-site location data is subject the Fourth Amendment protection because it could reveal intimate details about the subscriber's private life. Defendants Hazel, Pittman, and Brown argue the Government must receive a warrant based on probable cause to obtain historical cell-site location records, and any disclosure based on any lesser showing, including the "reasonable grounds" standard permitted by § 2703(d), violates the Fourth Amendment and Federal Rule of Criminal Procedure 41.

To prevail on their Fourth Amendment claims, Defendants must first show they had a reasonable expectation of privacy in the historical cell-site location information collected pursuant to the §2703(d) orders. "A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." United States v. Miller, 525 U.S. 435, 442–44 (1976); Smith, 442 U.S. 735, 743–44 (1979). "[W]hen an individual reveals private information to another, he assumes the risk that this confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." United States v. Jacobsen, 466 U.S.

109, 117 (1984). Under the third-party doctrine, courts have consistently held that individuals lack a reasonable expectation of privacy in basic telephone records. See Smith, 442 U.S. at 745 (holding defendant did not have a reasonable expectation of privacy in the phone numbers dialed); United States v. Clenney, 631 F.3d 658, 666 (4th Cir. 2011) (holding no privacy interest in basic subscriber information); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993) (holding no privacy interest in telephone records).

Although the Eighth Circuit and United States Supreme Court have yet to decide this issue, the circuit courts which have ruled the issue have uniformly concluded that defendants have no reasonable expectation of privacy in historical cell-site data.[3] United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016)(en banc), petition for cert. filed (U.S. Sept. 26, 2016) (No. 16-6308);[4] United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016), cert. granted (U.S. June 5, 2017) (No. 16-402) ("for the same reasons that Smith had no

[3] Defendants claim there is a circuit split on this issue, directing the court to United States v. Caira, 833 F.3d 803 (7th Cir. 2016) petition for cert. pending (filed Sept. 11, 2016) (No. 16-6761). Caira did not address whether the third-party doctrine applied to historical cell-site location information. Instead, it examined the issue of whether the third-party doctrine is implicated when an internet user accesses and communicates his IP address to third-party websites. Caira discussed the active debate regarding the current relevancy and application of the third-party doctrine to new technologies, (see id. at 807–809), ultimately holding the third-party doctrine did apply and that an internet user does not have a reasonable expectation of privacy in his IP address. Id. at 809. As such, Caira does not create a "circuit split" on the issue before this court.

[4] When the undersigned previously examined this same issue a little over a year ago, (see United States v. Hudson, 4:15cr3078, 2016 WL 1317090 (D. Neb. Feb 19, 2016)), a circuit split existed; the Fourth Circuit had held that a cellphone user has a reasonable expectation of privacy in historical cell-site location information. See United States v. Graham, 796 F.3d 332 (4th Cir. 2015). But upon rehearing en banc, that panel decision was vacated, with the Fourth Circuit now holding that "individuals do not have a reasonable expectation of privacy in historical [cell-site information] records that the government obtains from cell phone service providers through a § 2703(d) order." Graham, 824 F.3d at 428.

expectation of privacy in the numerical information at issue [in Smith], the defendants have no such expectation in the [cell-site information] here"); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015)(en banc) (holding that the defendant has no "objectively reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls."); In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding that the Fourth Amendment is not implicated when the government utilizes "Section 2703(d) orders to obtain historical cell-site information."); see also United States v. Guerrero, 768 F.3d 351, 359–60 (5th Cir. 2014); Jones, 908 F. Supp. 2d at 211; United States v. Ledbetter, 2015 WL 7758930, * 12–13 (S.D. Ohio Dec. 2, 2015); but see In re Application of US for order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010)(finding a 2703(d) order for historical cell-site data valid, but rejecting government's third-party doctrine argument stating "[a] cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way.").[5]

Generally, these courts have concluded the third-party doctrine applied when examining requests for historical cell-site information because the defendants (1) voluntarily conveyed their information to the cell phone company; and (2) the companies maintain that information in the ordinary course of business. See Carpenter, 819 F.3d at 887–89; Graham, 824 F.3d at 427–28; Jones, 908 F. Supp. 2d at 211. In Guerrero, the Fifth Circuit reasoned, "cell phone users voluntarily convey information to their service

[5] For an extensive list of previous cases holding that there is no reasonable expectation of privacy in historical cell-site records, see Jones, 908 F. Supp. 2d at 211 n.9.

providers . . . and '[they] understand that their service providers record their location information when they use their phones.'" Guerrero, 768 F.3d at 358 (citing In re Application, 724 F.3d at 613). These courts have also distinguished the disclosure of "non-content information" and "content information" concluding that historical cell-site data is non-content data which is provided less, if any, Fourth Amendment protection. See Carpenter, 819 F.3d at 886–89 ("[C]ell-site data—like mailing addresses, phone numbers, and IP Addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search.").

Defendants argue this court should follow the example of courts which have held that a cell phone user has a reasonable expectation of privacy in his or her historical cell-site location information. See In re Tel. Info. Needed for a Crim. Investigation, 119 F.Supp. 3d 1011, (N.D. Cal. July 29, 2015); Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2013). The defendants argue that cell phones have become an integral part of life for most American citizens and that by obtaining large volumes of historical cell-site location data for the defendants' phones, the government converted Defendants' phones into "virtual trackers" revealing specific and personal details of their lives and everyday activities.

Defendants' analysis and much of the case law on which their argument relies encompass cases in which the government sought warrants to track a defendant's movements, whether through the use of GPS devices or trackers. But as fully explained in Carpenter, use of cell-site data to determine a suspect or defendant's location significantly differs to that of GPS and trackers:

> GPS devices are accurate within about 50 feet, which is accurate enough to show that the target is located within an individual

> building. Data with that kind of accuracy might tell a story of trips to "the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on[.]" [United States v. Jones, 565 U.S. 400, 415 (2012)] (Sotomayor, J., concurring) (internal quotation marks omitted). But here the cell-site data cannot tell that story. Instead, per the undisputed testimony at trial, the data could do no better than locate the defendants' cellphones within a 120- (or sometimes 60-) degree radial wedge extending between one-half mile and two miles in length. Which is to say the locational data here are accurate within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate than the GPS data in Jones. And cell phone locational data are even less precise in suburban and rural settings. Areas of this scale might encompass bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque.

Carpenter, 819 F.3d at 889; (See also Gov. Exh. 9)(FBI Special Agent Kevin R. Horan's statement regarding the use and accuracy of historical cell-site data).

The court finds the same locational data accuracy is implicated in this case: historical cell-site data can show only an individual's approximate location while GPS monitoring reveals a precise and near exact location.[6] (Id.) As evidenced in the provided exhibits, the government relied on cell-tower use as far as seven miles from the robbery location to conclude that the specific defendant was active in the locational vicinity of the robbery. (See Def. Exh. 3). Had the government instead gathered the defendant's data through the use of a GPS device, the data could have shown the defendants' near exact locations at the time of the robberies, thus implicating more serious privacy concerns.

---

[6] In fact, according to Special Agent Horan, an individual's cell phone will always connect to the tower that has the strongest signal not necessarily the tower that is closest in location to the cell phone user. (See Gov. Exh. 9). This fact further complicates any attempt to pinpoint an individual's exact location based on his cell-site information alone.

The defendants argue further that cell-site location data gathered over an extensive period of time is more intrusive than the GPS tracker used in Jones because it allows the government to observe the defendants' movements for long periods of time. See 565 U.S. 400 (2012). While the court acknowledges the defendants' historical cell-site location information was gathered for extensive periods of time—the court ordered 388 days of data for Hazel; 186 days of data for Pittman; 454 days of data for Brown (see Exh. 3A, 5A, & 7A)—the ATM robberies under investigation spanned from January 2014 to April 2016, a period lasting more than 800 days. And as discussed above, the quantity of data itself does not mean that the quality or type of information gathered was as intrusive or that it is afforded the same expectation of privacy as the GPS monitoring in Jones.[7]

Ultimately, the undersigned agrees with the reasoning and holding of the multiple circuit courts which have ruled on this issue. The use of a cellular telephone is only possible through its utilization of cell towers, primarily those closest to the cell phone. A cell phone user voluntary conveys her phone's information to the cell phone tower with the closest/strongest signal and the service provider collects, records, and ultimately bills the user for her cell phone use in the ordinary course of business. While Defendants argue that the third-party doctrine should not apply because cell-site location information is conveyed only to the service provider and not the public, this distinction is irrelevant. In Smith, the Court held the third-party doctrine applied to telephone numbers dialed on a landline which, like a cellular telephone connection,

[7] In addition to GPS data being a far more precise and accurate manner to monitor an individual's movements, the court notes that GPS monitoring does not implicate the third-party doctrine in the same manner historical cell-site location information does. In Jones the government installed a GPS device directly to the defendant's vehicle to track his future movements. See 565 U.S. 400 (2012). In this case, the government received the defendant's historical cell-site location information through the third-party service providers' disclosure of business records which were collected and recorded in the ordinary course of providing service to the defendants.

conveys information only to the third-party service provider and the person receiving the telephone call. Smith, 442 U.S. at 745.

The court finds defendants have no reasonable expectation of privacy in their historical cell-site location information collected pursuant to the court's 2703(d) orders. Defendants' Fourth Amendment rights were not violated and the information obtained pursuant to those orders must not be suppressed.

The Government requested § 2703(d) court orders to obtain the historical cell-site information collected as a result of Defendants' cell phone use. (Exhs. 3A, 5A, and 7A). The SCA, and specifically § 2703(d), permits historical cell-site information to be disclosed pursuant to a court order based on "reasonable grounds," without a showing of probable cause. Defendants do not claim the government's §2703(d) applications failed to state "reasonable grounds" for such orders, so absent declaring § 2703(d) unconstitutional, there is no legal basis for excluding the historical cell-site information at issue in this case. Upon review of the evidence presented to the court and the prevailing law, the undersigned finds no basis for declaring § 2703(d) unconstitutional on its face or as applied. Accordingly, the motions to suppress filed by Defendants Brown, Hazel, and Pittman must be denied.

IT THEREFORE HEREBY IS RECOMMENDED to the Honorable John M. Gerrard, United States District Judge, pursuant to 28 U.S.C. § 636(b), that the motion to suppress filed by Defendants Brown, Hazel, and Pittman (Filing Nos. 134, 136, & 138) be denied in their entirety.

The defendants are notified that failing to file an objection to this recommendation as provided in the local rules of this court may be held to be a waiver of any right to appeal the court's adoption of the recommendation.

IT IS ORDERED that the jury trial of this case is set to commence before John M. Gerrard, United States District Judge, in Courtroom 1, United States

Courthouse, Lincoln, Nebraska, at 9:00 a.m. on September 18, 2017 or as soon thereafter as the case may be called, for a duration of ten (10) trial days. Jury selection will be held at the commencement of trial.

Dated this 23rd day of August, 2017.

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge